ADVANCES IN COMMUNICATIONS SECURITY

FOR

SPEECH AND DATA

A paper presented by J. M. K. Friend B.Sc.(Eng)
and E. W. Beddoes C.Eng., M.I.E.R.E.
Racal-Datacom Limited
at Racalex — September 1977

RACAL

RACAL-DATACOM LIMITED
Milford Industrial Estate
Tollgate Road, Salisbury
Wiltshire SP1 2JG, England
Telephone: 0722 23911
Telex: 477276

In this paper, the problems of securing both voice and data communications are considered. The need to protect voice communications has arisen only during the 20th century with the availability of reliable radio and telephone communications circuits, whereas man has felt the need to protect data in the form of the written word for more than 2,000 years.

In order to preserve the correct chronological order, data encryption is therefore considered first and it is shown how the basic operational requirements led to the design of today's modern electronic cipher communications security systems.

Most cipher techniques depend for their operation on the generation and synchronisation of long pseudo-random sequences and the design of a practical generator that may be used to produce such a sequence is given in outline. Finally, the special problems of voice encryption are considered and the various techniques that can be employed are detailed and their relative merits indicated.

The fundamental requirements of a data encryption system are as follows:-

1) The system should provide adequate security — what is adequate does, of course, depend not only on the nature of the data but also on the nature of the threat, that is the ability of the interceptor to both intercept and analyse the transmission. Systems that were thought highly secure, say, 50 years ago, can now be broken in a matter of minutes using today's computer analysis techniques.

2) The equipment should be simple to use — a device that is difficult to use will either be used wrongly or worse still, not used at all. In either event offering little or no security.

3) The device should be reliable in its operation, that is, its use should not impair the ability to communicate over an existing circuit. This may seem obvious, however, there have been a number of incidents in recent years which have been caused by cipher equipment failing to operate when most needed.

HISTORIC SOLUTIONS

As already mentioned, the data cipher has existed in one form or another for a very long time. One of the earliest examples of such a system was the Ceasar Alphabet which dates back to about 70 B.C. When using this system, each character of the plain text message is replaced with another character according to a 'look up table' as shown in Fig. 1.

Plain Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Plain Text	R	A	C	A	L	D	A	T	A	C	O	M	L	I	M	I	T	E	D
Cryptogram	U	D	F	D	O	G	D	W	D	F	R	P	O	L	P	L	W	H	G

Fig. 1 'Ceasar Alphabet'

Such a system is classified as a 'mono-alphabetic substitution cipher'. Substitution because a 'cipher' character is 'substituted' for each character of the plain text message and 'mono-alphabetic' as any given letter in the plain text is always replaced by the same character in the cipher text. Such a system offers little security as the statistics of the letter occurrence in the language of the original plain text can be applied to break the cipher. This weakness was partially overcome by the use of a polyalphabet substitution cipher, a version of which is exemplified by the Vigenere tableau shown in Fig. 2.

```
         C | C D E
         D |        etcetc
Key      E |
Alphabet F |
         G |
         H |
         I |
         J |
         K |
         L |
         M |
         N |
         O |
         P |
         Q |
         R |
         S |
         T |
         U |
         V |
         W |
         X |
         Y |
         Z | Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

Fig. 2 'Vigenere' Tableau

The technique here is very similar, however, the single cipher alphabet is replaced by a multiplicity of alphabets, different alphabets being used to encipher successive characters. The alphabet used is determined by a key, the longer this key, the greater the number of alphabets used and the more secure the system.

A further large improvement in security was obtained by the use of a 'one time' substitution system. The 'one time' system was, in effect, a polyalphabet substitution cipher in which the key length is equal to the length of the message. Provided that a key is used once and once only and is then destroyed, the system will be 'holocryptic' or unbreakable. That is, in order to decipher the resulting cryptogram, it is absolutely necessary to possess a copy of the key that was used to produce the cryptogram.

In practice, the 'one-time' system is implemented as shown in Fig. 3.

Placode	2 4 1 5 3	3 1 6 7 9
+Key	4 7 6 1 3	7 9 1 4 6
=Cipher	6 1 7 6 6	0 0 7 1 5
Cipher	6 1 7 6 6	0 0 7 1 5
–Key	4 7 6 1 3	7 9 1 4 6
=Placode	2 4 1 5 3	3 1 6 7 9

Fig. 3 'One Time Pad'

The plain text message is first converted by means of a 'look up table' to a sequence of decimal digits known as the Placode. To these are added without carry a second string of digits called the 'key', selected sequentially from a 'pad' of key material. The result of this addition is the cipher text. In order to decipher the message, it is necessary only to subtract the same 'key' from the cipher text in order to obtain the Placode. The key material is normally generated and provided as pads, each page being used once and then destroyed, hence the term 'one time pad'. It is, of course, not necessary to use the pages in order, a coded message can be preceeded by a plain language statement of the page and line number at which the key used starts. This does not reduce the security of the system as knowing the position of the key within the pad is of no assistance to an interceptor not in possession of the pad. Note that the cipher text is arranged as groups of five numbers separated by a space — this 'formatting' of the cipher text will ensure that a character added or missed is obvious when the cipher is transcribed. This is important as it can be seen that if the cipher text and the key get out of step, the deciphered text will be completely wrong.

Although offering the ultimate security, there are severe practical difficulties associated with the use of such a system.

Firstly, the generation of sufficient truly random key material to cope with a significant volume of traffic.

Secondly, the distribution and control of the key material, for it must be remembered that net security is lost if one pad is stolen and new pads must be distributed before the system can be used again.

The third difficulty is the tedious nature of the pencil and paper coding technique. This objection can and was overcome to some extent by the use of mechanical or electronic adding techniques and the use of punched paper tape instead of written pads as the source of the key material.

This also made possible 'on line' operation, that is the enciphering/deciphering of data in real time. It is worth noting that in this case, it is no longer necessary to ensure that the characters of the cipher text are rigidly formatted, provided other steps are taken to ensure that synchronisation between the cipher text and key are maintained.

The object of a cipher machine whether mechanical or electronic, is not to improve on the security offered by a 'one time' pad as that is not possible, but to very closely approach that level in a form that is much easier to use. Mechanical cipher machines, although still in use, have now been largely superseded by electronic systems that can be designed to offer high security, more user facilities and much improved reliability.

ELECTRONIC CIPHER MACHINES

Although several different techniques can and are employed to encipher the data in electronic cipher machines, this paper considers only the system that most closely emulates the operation of the 'one time' pad, and is of general application, that is, the additive cipher.

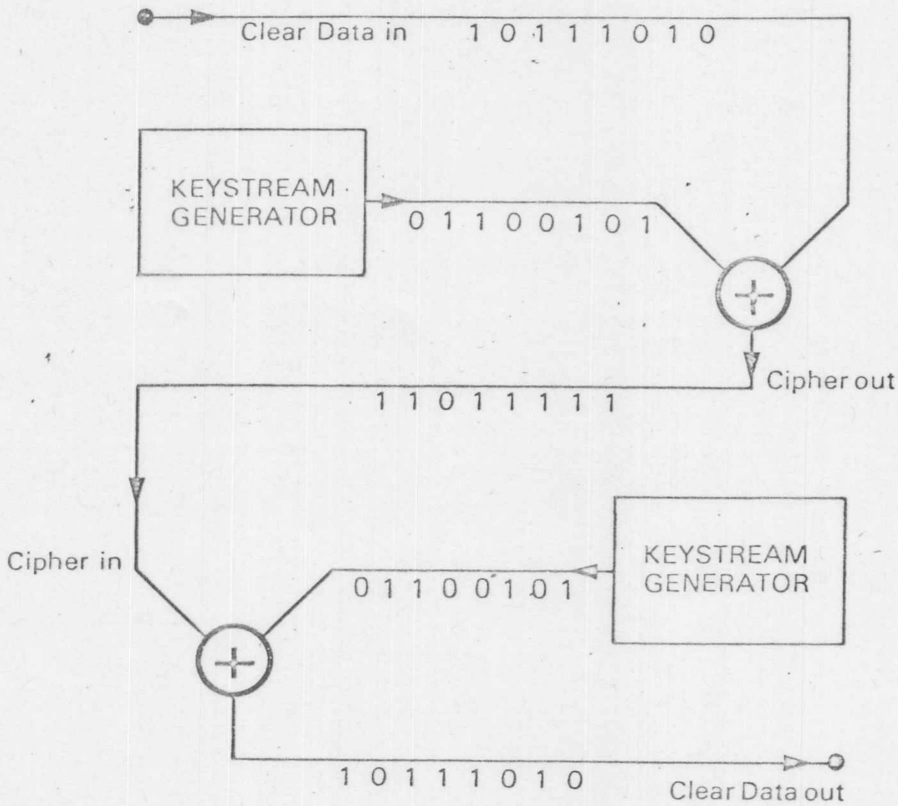

Fig. 4 Additive Cipher

In such a system, the plain text is once again converted to Placode, but this time into a stream of '1's and '0's, instead of a sequence of decimal digits and added without carry using modulo 2 addition to a key, also in the form of a 'Binary' stream, provided, not from a pad but from a device known as a "Keystream Generator". Note that in modulo 2 operation, addition and subtraction are interchangeable and, therefore, the deciphering process consists of once again adding the key to the cipher text.

A characteristic that is unique to this additive type of enciphering system is that it offers zero error extension. This means that if one character of cipher text is corrupted in the transmission process from the encryption terminal to the decryption terminal, the result will be that only the corresponding character of the deciphered plain text output will be corrupt. Thus, the introduction of such a cipher system does not degrade the error rate achieved over an existing channel in the clear mode. This is of particular importance where the transmission system used offers only modest error rates as, for example, in the case of HF SSB radio operation in poor propogation conditions.

KEYSTREAM GENERATORS AND KEY SETTINGS

It is appropriate at this point to consider the practical implementation of the keystream generator which is required to produce a repeatable random or pseudo-random sequence of '1's and '0's.

A simple keystream or pseudo-random binary generator can be formed by applying the appropriate modulo 2 feedback around an 'n' stage shift register which is stepped on by means of an external clock as shown in Fig. 5.

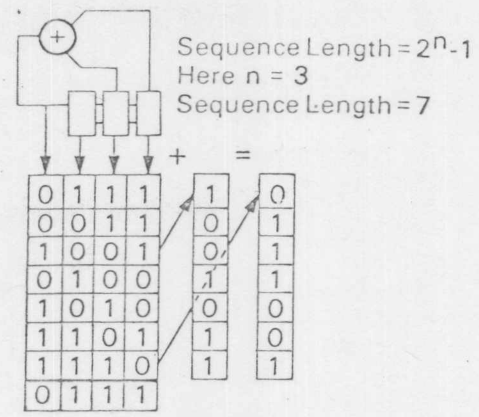

Fig. 5 Simple Keystream Generator

Using such a technique, the length of the sequence produced will be $2^n - 1$ provided that the correct stages of the register are used to provide the feedback and it is obvious that very long sequences can be produced using only a modest number of register stages. The sequence length is important as it must be remembered that the design aim is to produce a system analogous in operation to the 'one time' pad mentioned earlier. The keystream must, therefore, be long enough to allow all the messages to be processed during the operational life of the system to be enciphered using a different section of keystream.

It is obviously possible to start the pseudo-random binary generator or PRBG at any point on the output sequence by pre-loading the shift register with the appropriate pattern of '0' and '1's, this pre-load is normally referred to as the key setting. The key setting can in addition determine the feedback arrangement also, therefore, determining both the keystream in use and the position on that keystream.

Remember that, ideally, each message should be enciphered using a different section of keystream. To achieve this, a different key setting is required each time the PRBG is used. One way of achieving this is to form the key setting from two component parts, a Base Key which is loaded into the equipment and changed, periodically and a message key which is added as a preamble to the message and used to modify the base key such that messages enciphered using the same base key but different message keys utilise different sections of keystreams. This, then, is analogous to prefixing the enciphered message with the page and line number of the start of the key used when employing the 'one time' pad system.

The output sequence produced by a generator such as this has a number of interesting characteristics:-

1. The output is statistically flat, i.e '1' and '0' are equiprobable and randomly distributed. (In fact, the number of '0' = number of '1's$\pm$ 1 depending on whether the feedback is inverting or non-inverting.)

2. The result of adding a shifted version of the original to the original is to produce only another shifted version of the original.

A pseudo-random Binary Generator such as this is said to be linear, being a generator in which the describing equation (i.e. the equation that defines the output bits) is fixed and contains only simple addition of a function of the preceding 'n' output bits. (Where 'n' is the length of the generating register.) Because of this simple relationsHip between an output bit and the preceding 'n' bits, such a generator does not offer the resistance to determined attack usually required of today's cipher equipment.

The foreword equation must be made more difficult to invert and there are a number of ways in which this can be done:-

1. Change feedback taps dynamically.
2. Go outside GF2, i.e. other than mod 2 addition for the feedback logic
3. Change the foreword equation in other ways

In the case of 1. and 3. changes must be made at a rate such that $<n$ bits are output between changes. An example of a non-linear keystream generator embodying the desirable characteristics of a linear generator is shown in Fig. 6.

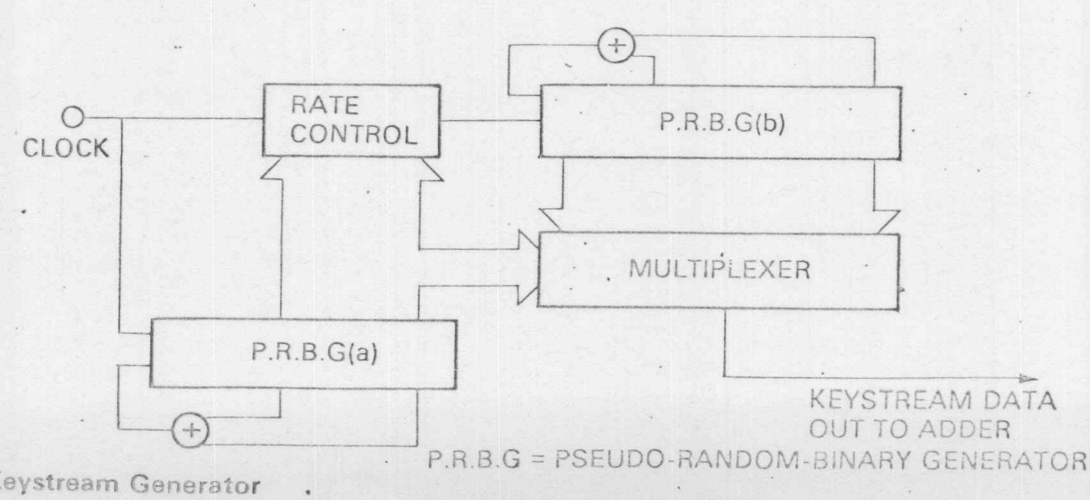

Fig. 6 Keystream Generator

The output of PRBG (a) is used to control both the number of times that PRBG (b) is moved on between output bits and also the stage of PRBG (b) that is used to provide the output. Provided that the number of clock pulses fed to PRBG (b) during one complete cycle of PRBG (a) has no common factors with the cycle length of PRBG (b) the final output will be a single sequence of length $(2^{n(a)}-1)(2^{n(b)}-1)$.

Such a non-linear generator does not share the linear generator's property of producing only another shifted version of itself when added to a shifted version of itself. This then can be used to great advantage for simply adding the outputs of two identical generators producing sequence lengths of 2^n will produce a system that is capable of producing different non-linear sequences each of length 2^n. By combining larger numbers of generators a formidable set of numbers can be built up.

The Racal-Datacom approach to keystream generator design was to configure a basic non-linear sequence generator producing a sequence of moderate length ($>10^{12}$) and then implement that generator as a large scale integrated circuit.

A number of these basic generators are then combined to produce a multiplicity of non-linear keystreams of considerable length.

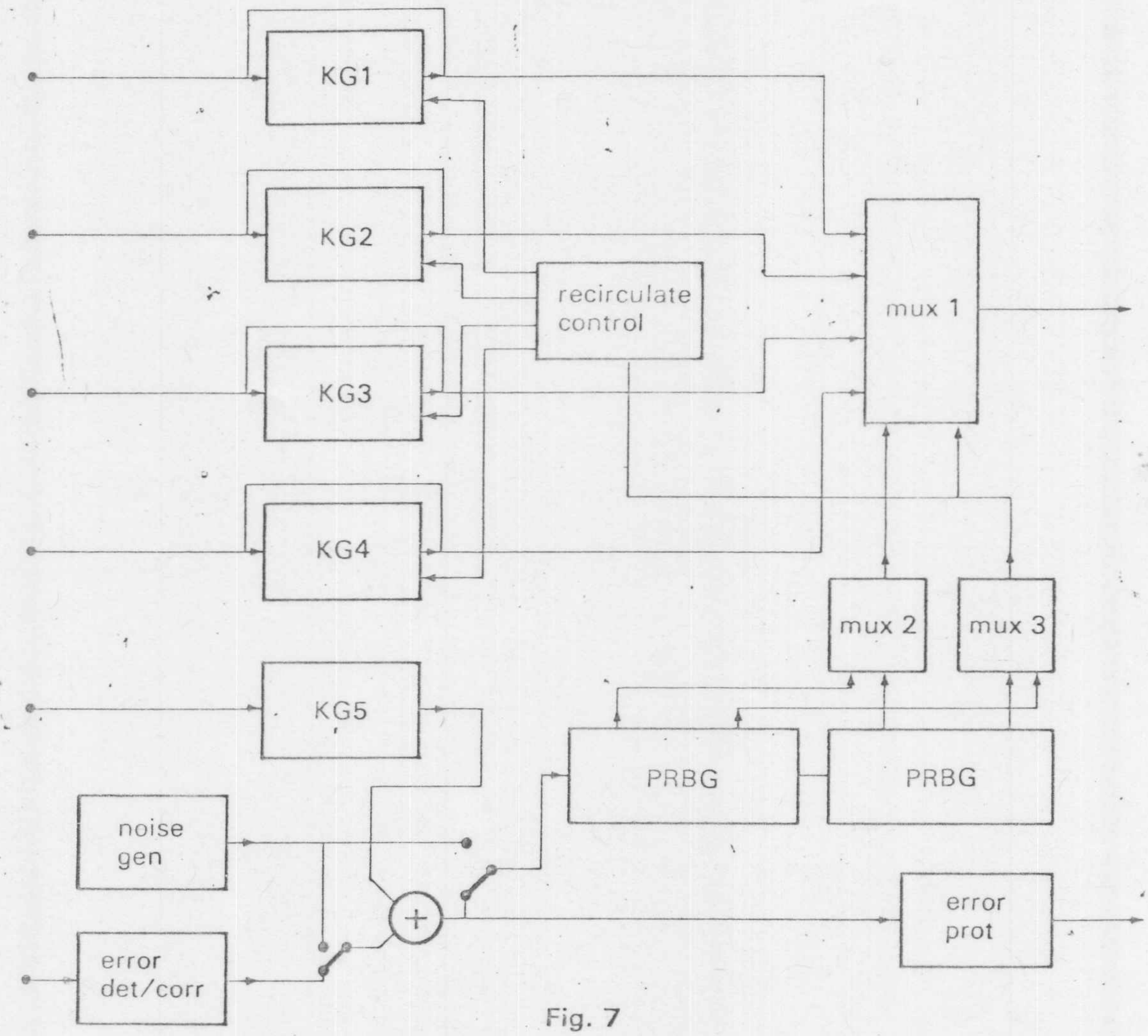

Fig. 7

The Fig. 7 shows an example of such a generator for use in an On-Line and Off-Line cipher and has the following characteristics:-

Base Key Setting	1.9×10^{45}
Number of Keystreams	1.3×10^{36}
Keystream Cycle length	7.4×10^{22}
Message Keys	6.9×10^{10}
Customer Options	3.4×10^{10}

Just to give some idea of the meaning of numbers of these magnitudes — if this keystream generator were started on one of its 10^{36} keystreams, it would take $10^6 \times 10^6$ years to use the full length of that one sequence, assuming it were used at the rate of 1,000 bits per second.

So much then for the basic additive enciphering process. There is, of course, much more to a cipher equipment than the keystream generator that is used to effect the process. The keystream synchronisation and data control systems employed in the equipment determine both the ease and reliability of operation of the equipment. In these areas, the advent of the microprocessor has permitted dramatic improvements in performance as well as permitting increasing sophisticated equipments to be implemented without excessive component counts, thus leading to improved reliability.

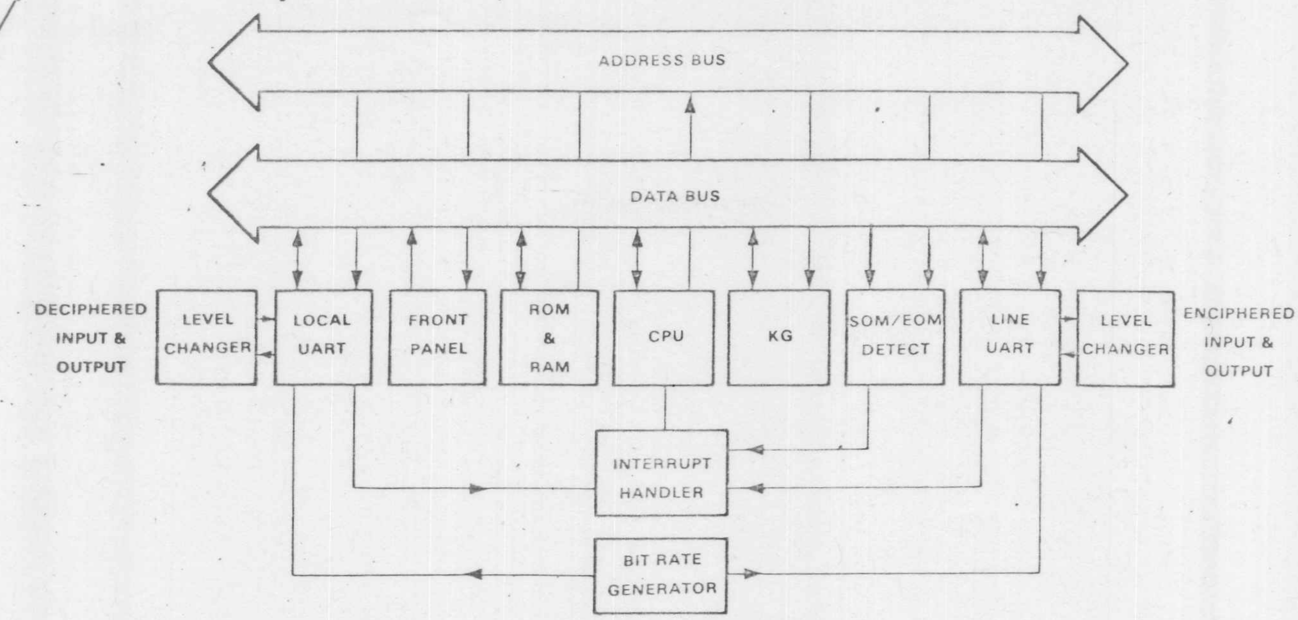

Fig. 8 'On Line Cipher'

The use of an 8-bit microprocessor in Racal-Datacom's current cipher equipment, the MA 4240 has made possible an equipment that can operate in a formatted off-line or an unformatted on-line mode under front panel control. In the off-line mode, the cipher text is formatted in 5 letter groups, 10 groups per line and this format automatically checked at the decipher terminal.

In the on-line mode the application of forward error correction to the message key ensures that the Encryption and Decipher keystream generators synchronise reliably. They are then maintained in synchronisation by stepping each under control of its own crystal clock. Although all character combinations can and will appear in the output cipher text, the flexibility conferred on the equipment by the microprocessor based design allows any combination that may be interpreted as a control code by the bearer system to be barred from the output cipher text.

If this combination occurs due to the enciphering process, the enciphering equipment will automatically replace it with another permitted combination. Such an equipment employing an additive technique can with suitable keystream generator design offer both a highly secure and convenient way of protecting plain text.

VOICE ENCRYPTION

The same technique can, of course, be used to encipher any data, provided that that data is first converted to a serial binary stream. Voice is a possible source of input data, it must first be converted to a binary stream by applying it to a suitable analogue to Digital converter, then enciphered using additive cipher techniques.

On receipt, the cipher is deciphered as previously described and the resulting data stream used to reconstitute the original voice input by applying it to a complementary Digital to Analogue converter as shown in Fig. 9.

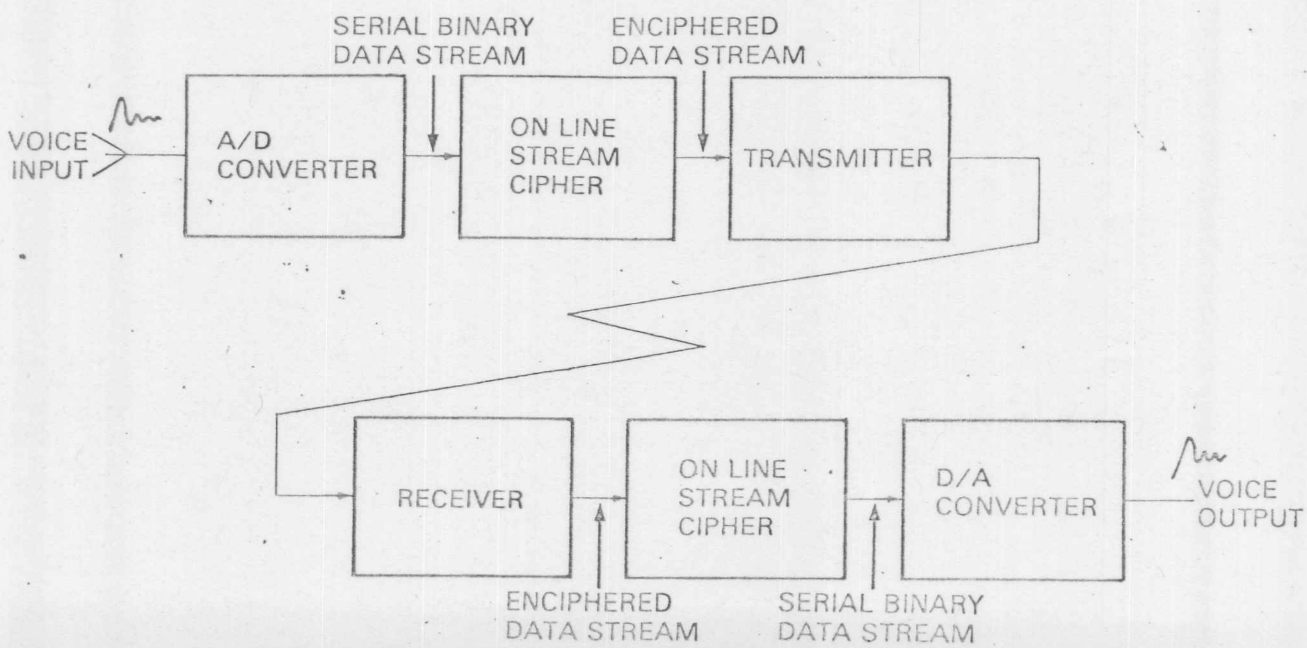

Fig. 9. 'Voice Cipher'

High rates will give high quality but are difficult to transmit. However, rates as low as 16k bits will give adequate speech quality with voice recognition.

16k bit is the highest rate which can be achieved by a 25kHz channel spacing VHF or UHF radio, due to IF bandwidth limitations. These radios often have such a system built in.

The straightforward simplicity of the digital system is evident from the figure and it is unfortunate that it is not suitable for transmission over speech bandwidth without employing some more special techniques.

Digital speech over normal voice bandwidth at bit rates as low as 2.4k bits is possible. However, the reduction in bit rates requires: Analysis of speech in real time to obtain its basic parameters: The transmission of these controlling parameters and real time synthesis of speech at the receiver.

The vocoder is such a system.

Its use where a large number of channels have to be secured is generally considered unacceptable on the grounds of its large physical size, cost and complexity. For these reasons, this method will not be considered further in this paper.

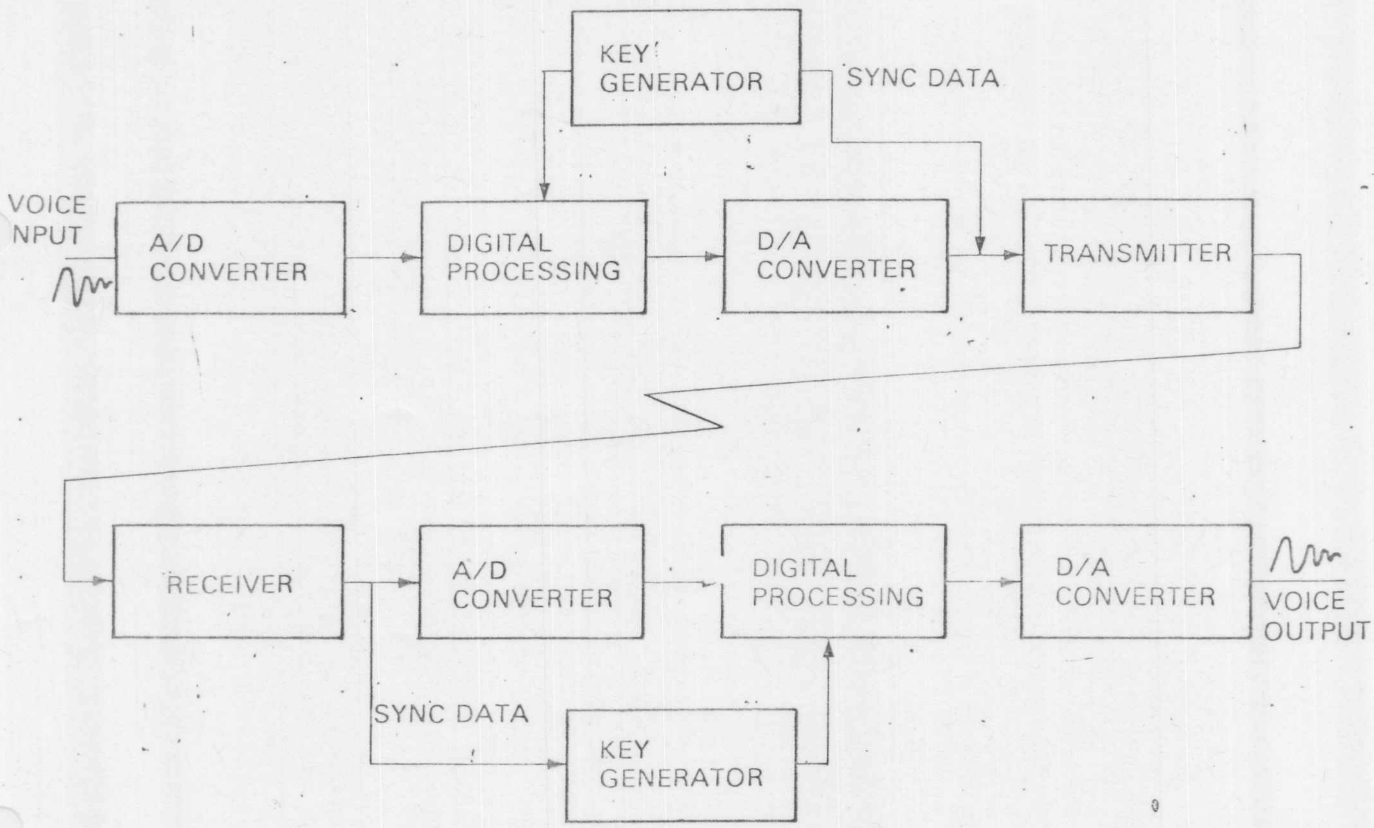

Fig. 10. Analog Speech Encryption System

ANALOGUE TECHNIQUES

Fig. 10 shows an alternative analogue solution to the problems of encryption of speech in which speech processing is usually done in digital form at very high rates which ensures a low level of noise and distortion in the encryption process and the final signal is converted back into analog form for transmission. At the receiver the signal is subjected to a similar process to reconstitute the clear speech.

It is a feature of such techniques that the encrypted signal occupies the same bandwith as the input signal and can, therefore, usually be transmitted over normal speech channels.

In general the levels of security attainable using analog encryption are determined by two factors:

a) The Keystream Generator

b) The voice processing arrangements

The first of these has already been covered and the latter will now be considered. Speech exists in three dimensions Vis.

Amplitude — Frequency — Time

In order to render speech unintelligible, the normal relationship between the three elements of a speech wave must be disrupted at a rate which is higher than the basic language information rate.

The disruption process must, however, continuously be changing to discourage the interceptor from using a simple systematic approach to listening.

Changing the amplitude of speech provides no security. It is, therefore, necessary to process in either the time domain, the frequency domain or both.

THE TIME DOMAIN

If a finite passage of speech is divided into unrecognisably short time elements and then rearranged in a random sequence under the control of a key generator, almost total disruption of the information occurs.

If the passage or frame of speech is long enough, and the elements (or segments) short enough, there are a large number of possible rearrangements which are unintelligible.

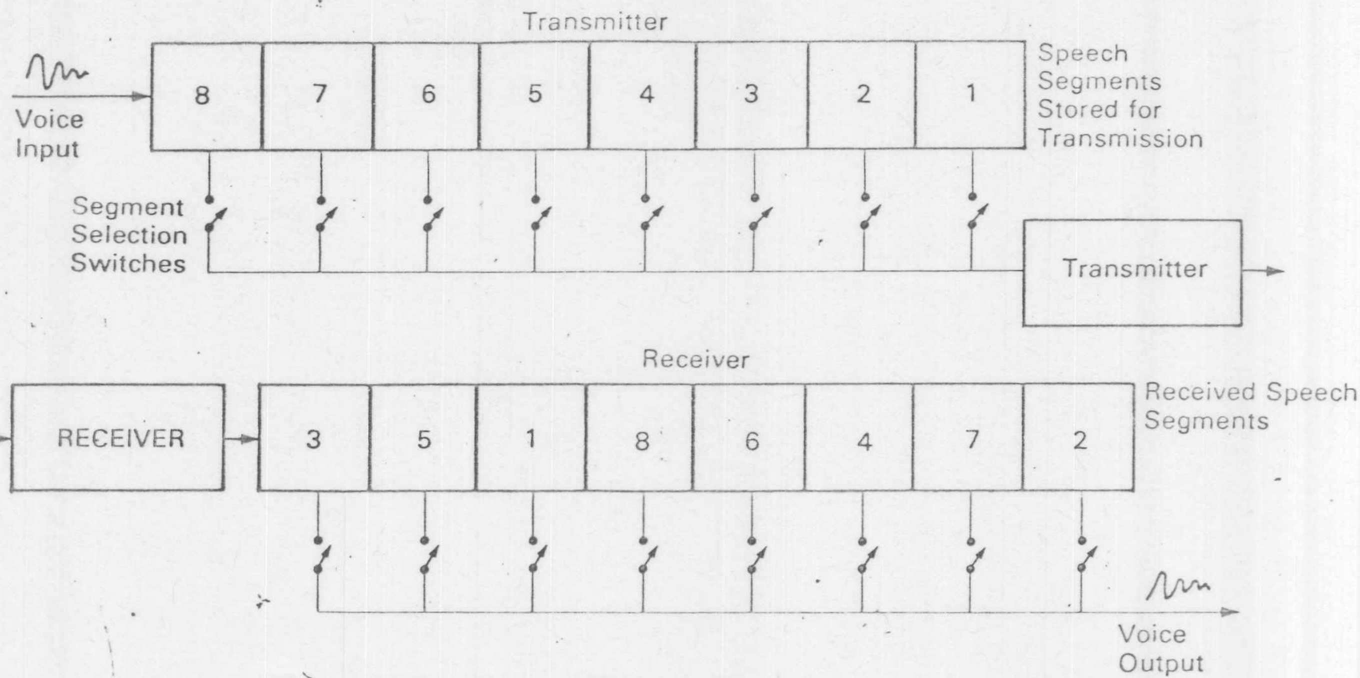

Fig. 11. Time Division Principles

Speech in sampled form is first stored in a 'frame' register which is eight segments long. These segments are selected one at a time in a pattern differing from the original and known to be unintelligible and transmitted.

At the receiver the process is reversed to assemble the segments in the original order. Eight segments can be rearranged in 40 thousand (8!) different ways.

However, many of these cannot be used because they are intelligible.

A mathematical basis for selecting patterns which can be understood has been determined. It operates as shown in Fig. 12.

Shift Function

1

1	2	3	4	5	6	7	8	
3	5	1	8	6	4	7	2	
2	+3	+2	+4	+1	+2	+0	+6	=20

Average Shift = $^{20}/_{8}$ = 2.5

2

1	2	3	4	5	6	7	8	
2	8	6	3	7	4	5	1	
1	+6	+3	+1	+2	+2	+2	+7	=24

Average Shift = $^{24}/_{8}$ = 3

Mutual Shift

3	5	1	8	6	4	7	2	
2	8	6	3	7	4	5	1	
1	+3	+5	+5	+1	0	+2	+1	=18

Average Mutual Shift = $^{18}/_{8}$ = 2.25

Fig. 12. Calculation of Shift Function

If the segments are numbered 1 to 8 and the transmitted order is compared with the original order, the average shift is calculated as the mean displacement of segments from their original natural position.

The rearranged pattern can be compared with all the other patterns and the average mutual shift calculated in the same way.

High absolute values of shift are necessary to ensure low intelligibility to the interceptor listening in clear.

High mutual values of shift are necessary to ensure low intelligibility to the interceptor listening on a captured piece of equipment on the wrong setting.

The relationship between shift function and intelligibility has the following form, note that some residual intelligibility remains. However, this can be reduced to an insignificant level.

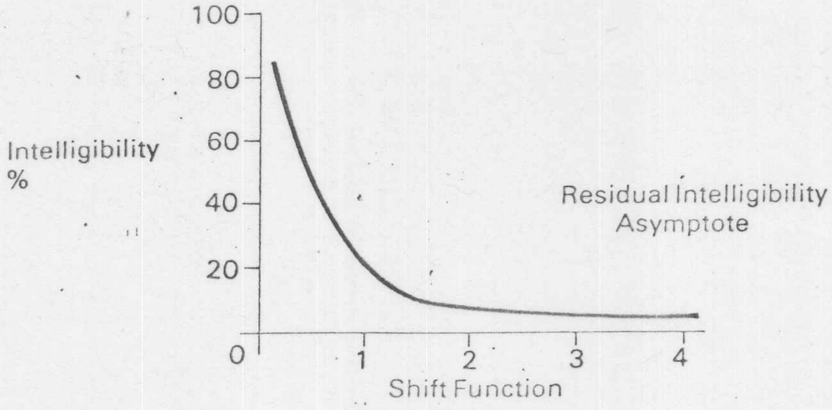

Fig. 13

All patterns used in Racal-Datacom equipment have been selected by a computer screening process to ensure a high absolute shift function and a high mutual shift function.

In order to decrypt the received signal, complementary patterns are used at the receiver.

These are stored in a Read Only Memory and selected under the control of a Key Generator.

Synchronisation of the key generators in the transm ter and receiver is necessary therefore, to ensure use of the correct patterns.

Synchronisation of timing relative to the received signal is also necessary. Having provided a method of disrupting speech in the time domain, we must turn our attention to the frequency domain.

FREQUENCY DISPERSION

The earliest and best known form of disrupting speech in the frequency domain is merely to invert the speech band using a modulation process. Since this is a fixed process it provides no security.

Slightly better is a method known as 'band scrambling' with inversion where the spectrum is split into a number of bands; generally 5 maximum which is the optimum choice. These are then rearranged in the frequency band, with or without frequency inversion. There are theoretically only 3,840 ways of doing this of which only about 12 are totally unintelligible and the cost in terms of hardware and complexity is considerable.

Racal-Datacom have, therefore, developed a different technique which we refer to as 'Frequency Dispersion'.

This has the effect of continuously varying the pitch of the frequency information contained in each of the eight segments produced by time division. It is achieved by varying the digitisation rate of the A/D and D/A converters in the transmitting unit and its effect removed by a similar process in the receiving unit.

One of its strengths is that the magnitude and direction of this pitch variation is a function of the key generator output and they both, therefore, change in a pseudo-random manner each frame.

A typical pattern of variation is shown in Fig. 14.

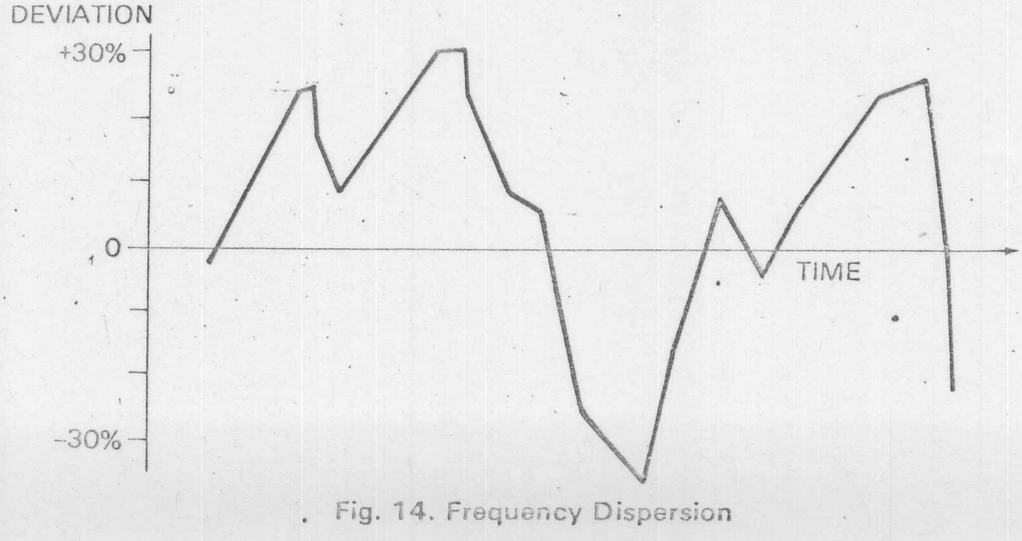

Fig. 14. Frequency Dispersion

It has a further advantage of varying the segment lengths and, therefore, the position of the segment boundaries, so considerably increasing the difficulty of an attack on the intercepted signal.

Both time division and frequency dispersion are combined in Racal analog encryption equipment to provide maximum resistance against systematic analysis and a minimum residual intelligibility.

SYNCHRONISATION

The need for synchronisation of sending and receiving units has already been referred to.

Synchronisation in analog encryption equipment is necessary for similar reasons:

a) For the key generators to be in step
b) For the segment and frame boundaries to be synchronous with received data.

Fig. 15 shows how this data is generated, used at the transmitter, applied to a modem and subsequently detected and used at the receiver. A synchronising preamble and a message key are transmitted to ensure the key generators are in step. When this is correlated at the receiver, it also produces timing data.

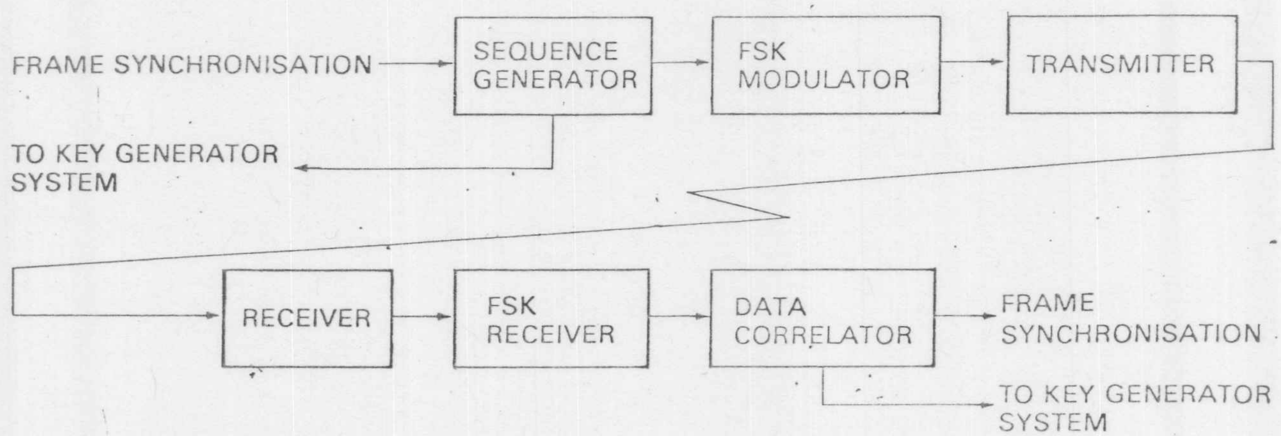

Fig. 15.

This information can either be sent continuously with the encrypted speech, or at the start of each transmission.

Continuous data has advantages not shared by initialising sync of:-

a) Late entry during transmission
b) Auto clear/secure switching controlled by sync data

It has the disadvantage also not shared by initialising sync, of having to share the power available between sync and speech and hence may produce a slight reduction in range.

The key generator once synchronised has a flywheel effect which lasts for about 30 minutes. This is more than adequate to cope with fading, etc. The system also allows for some propogation delay in the radio path without the need to frame re-synchronise.

OPERATIONAL REQUIREMENTS

It is interesting to consider the requirements of a voice encryption equipment to enable an assessment to be made of how well the foregoing techniques can meet them in a practical environment.

Fundamentally an equipment must:-

a) Communicate at least as well in the secure mode as in the clear
b) Allow voice recognition
c) Use existing channels
d) Allow late entry during a transmission with rapid synchronisation
e) Be cost effective and not unduly complex
f) Be simple, foolproof and automatic in operation

The comparison table Fig. 16 shows how the various techniques satisfy the foregoing requirements:-

REQUIREMENTS	SYSTEM		
	2.4k bits	16k bits	Analog
1. Clear-Secure equality	X	✓	✓
2. Voice Recognition	X	✓	✓
3. Can use existing channels	✓	X	✓
4. Late entry	✓	✓	✓
5. Cost-complexity	X	✓	✓
6. Operational simplicity	✓	✓	✓

Fig. 16. Comparison of Requirements and System Characteristics

The table Fig. 17 shows the compatibility of the various techniques with existing types of communications channels:-

	System: 24K BITS	16K BITS	ANALOG	
V.H.F. RADIO	Requires Group Delay Equalisation	Requires Special Radio	Satisfactory	Type of Channel
H.F. RADIO	Requires Expensive Modem	Not Possible	Satisfactory	
TELEPHONE	Requires Group Delay Equalisation	Not Possible	Satisfactory	

Fig. 17

In conclusion it can be said that a 16k bit digital system because of its intrinsic simplicity is superior to analog encryption where the channel bandwidth permits its use. When built into the radio it provides an optimum solution for portable equipment, one single package.

For existing HF radio or telephone systems an add on unit such as the MA 4224 is required. This is a continuous sync time and frequency domain encryption device giving operational flexibility and channel compatibility and embodying many of the features described.

It has also been shown how an additive cipher technique implemented using the pseudo-random sequence produced by a non linear Kg and used in conjunction with a flexible data control system offers a good general solution to the problems of data security.